

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Google LLC, MG Freesites Ltd, Amazon.com Inc.,
and Meta Platforms, Inc. Accounts,
Described in Attachments A-1 to A-4

Case No. MJ22-081

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Subject User Accounts, more fully described in Attachments A-1 to A-4, incorporated herein by reference.

located in the Northern and Central District of California and the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachments B-1 to B-4, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 2261A(2)(B)

Cyberstalking

47 U.S.C. § 223(a)(1)(E)

Repeated Harassing Communications

The application is based on these facts:

- ☒ See Affidavit of NCIS Special Agent Eddy Crochetiere, attached hereto and incorporated herein by reference.

- ☒ Delayed notice of 365 days (give exact ending date if more than 30 days: 03/02/2023) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Eddy Crochetiere
Applicant's signature

EDDY CROCHETIERE, Special Agent, NCIS

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/02/2022

S Kate Vaughan
Judge's signature

City and state: Seattle, Washington

S KATE VAUGHAN, United States Magistrate Judge

Printed name and title

1 providers of electronic communications services and/or remote computing services
 2 (collectively, “the providers”):

- 3 i. Google LLC, headquartered at 1600 Amphitheatre Parkway,
 4 Mountain View, California 94043 (“Google”);
- 5 ii. MG Freesites Ltd, parent entity of Pornhub, 195-197 Old
 6 Nicosia-Limassol Road, Block 1 Dali Industrial Zone, Cyprus
 7 2540 (“Pornhub”);
- 8 iii. Amazon.com, Inc., headquartered at 410 Terry Ave N, Seattle,
 9 Washington 98109 (“Amazon”);
- 10 iv. Meta Platforms, Inc., parent company of Facebook/Instagram,
 11 headquartered at 1601 Willow Road, Menlo Park, CA 94025
 12 (“Meta”).

13 3. The information to be searched is described in the following paragraphs and in
 14 Attachment A to each search warrant. This affidavit is made in support of an application for
 15 search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the
 16 providers to disclose to the government copies of the information (including the content of
 17 communications) further described in Section I of Attachments B to each search warrant.
 18 Upon receipt of the information described in Section I of Attachment B, government-
 19 authorized persons will review that information to locate the items described in Section II of
 20 Attachment B.

21 4. The facts set forth in this Affidavit are based on my own personal knowledge;
 22 knowledge obtained from other individuals during my participation in this investigation,
 23 including other law enforcement officers; review of documents and records related to this
 24 investigation; communications with others who have personal knowledge of the events and
 25 circumstances described herein; and information gained through my training and experience.
 26 Because this Affidavit is submitted for the limited purpose of establishing probable cause in
 27 support of the application for a search warrant, it does not set forth each and every fact that I
 28 or others have learned during the course of this investigation.

5. Based on my training and experience and the facts as set forth in this affidavit,
 there is probable cause to believe that violations of 18 U.S.C. § 2261A(2)(B) (cyberstalking)

1 and 47 U.S.C. § 223(a)(1)(E) (repeated harassing communications) have been committed by
 2 Christopher Scott CRAWFORD (C.S. CRAWFORD). There is also probable cause to search
 3 the information described in Attachment A for evidence of these crimes further described in
 4 Attachment B.

5 THE INVESTIGATION

6 6. On October 27, 2021, fourteen public-facing U.S. Navy email addresses
 7 received an email from the email address “crawford132@gmail.com,” with the display name
 8 of “Scott crawford.” As explained below, this email address is associated with subject
 9 Christopher Scott CRAWFORD (C.S. CRAWFORD). The email contained thirty-six nude
 10 and/or intimate digital photos of a young woman later determined to be C.S. CRAWFORD’s
 11 ex-wife K.C., a U.S. Navy service member. The email message identified K.C. by name and
 12 rank and alleged that she was a prostitute who solicited clients using the internet. Routine
 13 criminal records checks revealed that C.S. CRAWFORD had an extensive criminal history of
 14 stalking and threatening K.C. and those associated with her in violation of existing
 15 restraining orders. The criminal history included numerous police reports, several arrests,
 16 active restraining orders (in California, Texas, and Washington), and active arrest warrants
 17 (in California and Texas). C.S. CRAWFORD is known to reside in Everett, Washington,
 18 and, until recently, K.C. was stationed by the U.S. Navy in San Diego, California (K.C. was
 19 reassigned to a new duty station in January 2022, for her safety).

20 7. I conducted an initial interview with K.C. on November 2, 2021. During the
 21 interview, K.C. stated that, since their separation in approximately April of 2019,
 22 C.S. CRAWFORD has continually harassed her with phone calls, text messages, emails,
 23 social media messages, and gift messages appended to commercially delivered parcels, in
 24 defiance of restraining orders. K.C. stated that C.S. CRAWFORD would call her repeatedly
 25 – usually during inconvenient late-night hours – from his known cellular phone number as
 26 well as Google Voice phone numbers unknown to her. K.C. stated C.S. CRAWFORD’s
 27 communications primarily contained profane and lewd insults, disparaging remarks, and
 28 threats to “destroy” or “ruin” her. K.C. stated that C.S. CRAWFORD has repeatedly told her

1 that he would not stop harassing her until she killed herself. K.C. has changed her phone
2 number at least five times to avoid contact with C.S. CRAWFORD but he very quickly
3 discovers the new number and resumes harassing her. In addition, K.C. stated
4 C.S. CRAWFORD has told her that he provided her contact information and address to his
5 associates in prison.

6 8. K.C. stated that C.S. CRAWFORD has harassed and threatened other people
7 associated with her, including her mother, stepfather, grandfather, sister, divorce attorney, a
8 court-mandated psychologist, and various members of her command.

9 9. K.C. stated she was also aware of C.S. CRAWFORD distributing her intimate
10 images to her acquaintances and posting them on adult websites including the website
11 Pornhub. K.C. stated she consensually sent C.S. CRAWFORD the intimate images
12 approximately ten years prior. K.C.'s verbal descriptions of the photographs and their
13 backgrounds matched the set of images sent to the U.S. Navy inboxes.

14 10. K.C. stated the harassment sends her "into a panic," causes her to not be able to
15 "function," and has made her feel "anxious" and "paranoid." She stated she is "scared" of
16 C.S. CRAWFORD and in the past has "slept with the recliner pushed up against the door" in
17 case he was to break into her residence in the middle of the night.

18 11. After the interview, K.C. provided me with a data CD containing
19 approximately 246 digital files. These files consisted of portable document file (PDF)
20 exports, audio files, screenshots, and images documenting hundreds of harassing emails,
21 phone calls, text messages, social media messages, and voicemails appearing to be sent from
22 C.S. CRAWFORD to K.C., her family members, and her associates. Almost every
23 communication from C.S. CRAWFORD included insulting names, obscene language,
24 threats, and/or statements of his intent to embarrass, humiliate, scandalize, stalk, "ruin,"
25 "destroy," cause suffering to, cause mental illness to, and impoverish K.C. In one email,
26 C.S. CRAWFORD stated that if he were to "end up homeless" due to K.C.'s "bullshit"
27 (likely referring to K.C.'s multiple police reports against C.S. CRAWFORD), that she
28

1 “would not survive” his homelessness. C.S. CRAWFORD also stated in several
2 communications that he intended to torment K.C. until she killed herself.

3 12. I reviewed digital files obtained from K.C. documenting harassing text
4 messages and transcribed voicemails from phone number (512) 667-5926 to K.C. Based on
5 the content of the messages, they appeared to be from C.S. CRAWFORD, and a grand jury
6 subpoena to T-Mobile USA, Inc. for subscriber information for (512) 667-5926 revealed it to
7 be subscribed to “CHRISTOPHER CRAWFORD” at 8616 8TH AVE W, EVERETT, WA
8 98204.

9 13. Based on my interview with K.C. and my review of the digital files provided
10 by her, the Google email account “crawford132@gmail.com,” which is the same email
11 account from which the nude/intimate photos of K.C. were sent to fourteen public-facing
12 U.S. Navy email inboxes, was also the apparent sender of dozens of threatening and
13 harassing emails to K.C. and others associated with her. The following are examples of
14 messages from “crawford132@gmail.com” that I have reviewed:

- 15 • An email sent on June 10, 2020, to K.C. and the guardian ad litem appointed by the
16 Snohomish County Superior Court in connection with divorce proceedings, included
17 the following: “You have a very hard road ahead of you and I’m going to be
18 watching. One slip up, one instance of me thinking you are not fit to raise our
19 daughter and Im going to take Sam away from you. That is a fucking promise.”
- 20 • An email sent to K.C. on June 16, 2020, included the following: “I fucking hate you.
21 The only things keeping me going are knowing that doing so vexes you and to
22 someday watch you lose everything like I have.”
- 23 • An email sent to K.C. on June 22, 2020, included the following: “You wont be able to
24 hide behind this TEMPORARY protective order for much longer.”
- 25 • An email sent to K.C. on October 27, 2021, included the following: “Why would you
26 assume that your nude photos were only on one site? Every single time I miss my
27
28

1 daughter, I am going to make you suffer for it. Ask [M.N.¹] which one of your
2 misshapen tits he likes best, hes seen them many times.”

- 3 • An email sent to K.C. on October 27, 2021, included the following: “and you have 2
4 days to pay me 850 dollars AND have a visitation supervisor call me or I file 6
5 contempt cases against you. You worthless fucking whore, I amgoing to make sure
6 that you spend every single day hating that you were ever born.”
- 7 • A second email sent to K.C. on October 27, 2021, included the following: “and btw, I
8 sent multiple copies of ALL your nudes to kirkland in prison and told him to
9 distribute them to anyone he wanted. He also distributed your full name,social
10 security number, address and employment...you know, in case anyone is getting out
11 and wants to visit the cunt who he’s been jerking off to for a year.”
- 12 • An email sent to K.C. on October 29, 2021, included the following: “Just wanted to
13 let you know that I came across a porn ad to “fuck local singles” and they were using
14 one of your nudes in their ad. Isn’t that great?! Millions of people all over world, at
15 random, now have proof that you are a whore for as long as their is the internet. Does
16 it turn you on knowing that your father jerks off to you? Oh, did I forget to mention
17 that I sent all of your nudes to your pedophile family years ago? Fuck you cunt. My
18 goal in life is to make you kill yourself.”
- 19 • A second email sent to K.C. on October 29, 2021, included the following: “Tomorrow
20 I’m going to sell your SSN, your phone number, your email address and all your
21 personal history on the dark web. Just try and stop me, cunt.”
- 22 • A third email sent to K.C. on October 29, 2021, included the following: “I’m also
23 going to print out your nudes and mail them to every address within 5 blocks of you,
24 so all your neighbors know what a whore you are. I’m also working on getting the
25 email addresses for every chief in your command and guess what they will find in
26 their email? That’s right! Vulgar photos of a lying, cheating whore!”

27
28 ¹ M.N. serves as K.C.’s Command Master Chief.

- 1 • Another email sent to K.C. on October 29, 2021, included the following: “I am going
2 to ruin your life. I am going to make every breath you have ever drawn, wasted. I am
3 going to make sure you beg for a bus to run you over. And when your mental state
4 starts slipping even more, I am going to fight tooth and nail to have you disgraced,
5 comitted and then I am going to take [S.C.²] from you forever.”
- 6 • An email sent on November 9, 2021, and forwarded directly to me from K.C.,
7 included the following: “Keep trying, stupid, they wont stop me, they wont touch me,
8 but they will absolutely arrest you for kidnapping. I know you think youve gotten me,
9 im just letting you tighten the noose, cunt.”

10 14. A grand jury subpoena to Google for subscriber information for
11 “crawford132@gmail.com” revealed the email account to be subscribed to “Scott
12 Crawford,” with a verified phone number of (512) 667-5926 and an account identifier of
13 889486101222.

14 15. On November 24, 2021, Google was served with a preservation letter under 18
15 U.S.C. § 2703(f) related to the Google email account “crawford132@gmail.com.”

16 16. Based on my interview with K.C., and my review of emails provided to me by
17 K.C.’s stepfather, on or about November 3, 2021, a Facebook account with the display name
18 “Rick Johnston” was used to send to K.C.’s stepfather eight nude/intimate images of K.C.
19 consistent with the set of intimate images sent by “crawford132@gmail.com” to the U.S.
20 Navy inboxes.

21 17. A grand jury subpoena for information regarding the “Rick Johnston”
22 Facebook account (account number 100074078874761) revealed the email address
23 associated with the Facebook account to be the Google email account
24 “rickjohnston1888@gmail.com.” A grand jury subpoena to Google for subscriber
25 information for the “rickjohnston1888@gmail.com.” email account revealed Internet
26 Protocol (IP) address 2601:601:a300:4ab0:cd57:98ec:2a4a:6899 was used to log in to this
27

28 ² S.C. is the daughter of K.C. and C.S. CRAWFORD.

1 account on October 30, 2021, at 2:15 and 2:17 a.m. UTC. Information obtained pursuant to a
2 grand jury subpoena to Comcast Cable Communications for subscriber information for this
3 IP address revealed it to be subscribed to CHRISTOPHER CRAWFORD at
4 8620 8TH AVE W APT C, EVERETT, WA 98204-1640. Additionally, this same IP address
5 was used to log into Instagram account number 27235979350 (with account vanity name
6 “cscottcrawford”) on October 30, 2021, at 4:02 a.m. UTC. A grand jury subpoena for
7 information regarding this Instagram account was revealed to be registered to “Scott
8 Crawford” with the verified cellular phone number of (512) 667-5926.

9 18. I have received a copy of an Agreed Protective Order, number 2012-C1-15792,
10 issued by the District Court of Bexar County, Texas, dated October 11, 2012, which protects
11 K.C.’s mother, stepfather, and sisters from communication or harassing conduct by
12 C.S. CRAWFORD. The order stemmed from an inconclusive police investigation into
13 C.S. CRAWFORD’s alleged sexual molestation of K.C.’s 10-year-old sister, C.B. The order
14 states that it is in effect for the lifetime of C.S. CRAWFORD, states that C.S CRAWFORD
15 appeared at the hearing in person, was represented by an attorney and agreed to the order,
16 and is signed by C.S. CRAWFORD’s attorney. The sending of the nude/intimate images of
17 K.C. via the “Rick Johnston” Facebook account appear to be a violation of this order.

18 19. Based on my review of the digital files provided by K.C., the user of Google
19 Voice phone number (401) 615-4218 has repeatedly called K.C.’s cellular phone and at least
20 once has left a voicemail with disparaging remarks. A grand jury subpoena to Google for
21 subscriber information for this Google Voice phone number revealed it to have the Google
22 Account ID 889486101222, and to be registered to “Scott crawford” with a true phone
23 number of (512) 667-5926. The same Google Account ID is also the account identifier for
24 the “crawford132@gmail.com” Google email account.

25 20. Based on my review of the digital files provided by K.C., the Google Voice
26 phone number (786) 904-3683 has sent lewd text messages to the cellular phone of J.M, one
27 of K.C.’s U.S. Navy coworkers. I have reviewed saved images of the text messages sent to
28 J.M. The text messages contained lewd insults and two nude/intimate images of K.C. that

1 appear to be from the set of nude/intimate images sent by “crawford132@gmail.com” to the
2 U.S. Navy inboxes. Among other things, the sender of the messages stated, after sending one
3 of the photos, “These pictures are being sent all over the navy, to her command, her
4 coworkers, her former shipmates, even the secretary of defense.” After sending another of
5 the nude/intimate photos, the sender stated, “Don’t worry, I don’t care if you save the pics
6 and jerk off to them...I sent her pictures and address to prison inmates for exactly that
7 reason, and frankly, if I was married to your wife, I’d be looking everywhere else as well.”
8 After being advised by J.M. that if the sender continued to make contact with him or any
9 member of his family, he would be contacting the police and filing a report for harassment
10 and distributing pornographic images without consent, the sender responded by texting,
11 among other things, “Call the cops, please, they won’t do a fucking thing, just ask [K.C.]
12 how much she was able to stop me.” After threatening to ruin J.M.’s career, the sender
13 replied, “And thanks to your empty shit talk, I am going to track down and contact every
14 single member of your family I can find.” A grand jury subpoena to Google for subscriber
15 information for Google Voice phone number (786) 904-3683 revealed it to have Google
16 Account ID 456326907605, and to be registered to “Christopher crawford” with a recovery
17 email of “crawford132@gmail.com” and a recovery cellular phone number of (512) 667-
18 5926.

19 21. The same grand jury subpoena revealed this Google Voice number called
20 K.C.’s cellular phone three times and sent one text message on October 29, 2021. I have
21 obtained a certified copy of a Criminal Protective Order issued by the Superior Court of
22 California, County of San Diego, restraining C.S. CRAWFORD from having any personal,
23 electronic, telephonic, or written contact with K.C., with exceptions only for the safe
24 exchange of children and court-ordered visitation. The order indicates that C.S.
25 CRAWFORD was served with a copy of the order at the hearing, and that it was issued on
26 June 22, 2021, and expires three years from the date of issuance. At the time of the calls and
27 text message in October 2021, the protective order was in effect, and K.C. had custody of
28 S.C. and was residing in California, while C.S. CRAWFORD was residing in Washington.

22. I have received and reviewed nine images and 28 digital audio files provided by U.S. Navy Master Chief Petty Officer M.N., who is K.C.'s Command Master Chief. M.N. stated to me that he began receiving calls from C.S. CRAWFORD in approximately April 2021, and that the calls were initially polite until M.N. refused to assist C.S. CRAWFORD by forcing K.C. to provide money and other considerations, after which C.S. CRAWFORD began using obscene, lewd, and insulting language toward M.N. The images and recordings I reviewed documented text messages sent to M.N. from (512) 667-5926, the T-Mobile phone number associated with C.S. CRAWFORD, and (786) 904-3683, the Google Voice phone number associated with C.S. CRAWFORD, along with voice mail messages. One of the images I reviewed appeared to be a string of undated text messages from (786) 904-3683 to M.N.'s personal cell phone. The sender sent an image file that appears to be one of the intimate photos of K.C. sent by C.S. CRAWFORD to U.S. Navy inboxes. Following the photo, the sender sent several text messages that included the following: "Don't worry, most of the navy around the world is receiving these pictures," and "I am going to destroy her and do everything I my power to make her kill herself. I've already sent her nudes and address to some friends of mine in prison, they are going to be visiting her for some fun when they get out, im sure. I'm also selling her social, birthrate, name, address, and all military paperwork I have from 10 years with her on the dark web." Among the text messages from (512) 667-5926 that were sent to M.N.'s government cell phone were the following:

- "Petty officer [K.C.], who bragged on the record about making chief, is an internet portn star and for the rest of her life, her friends, family and employers will receive links to the dozens of websites that contain her photos and videos and they all identify her by name, rank and rate."
- "I'm going to make it so that her being in the military is a liability to the US government. I may even decide to list the classified material that the idiot left behind...who knows? Point is, as long as she has my daughter, she will live in hell."

- 1 • “Point is, [K.C.] will be sending me 75% of her pay and retirement for the rest of her
- 2 life. When she can no longer feed my daughter, I will take custody and watch happily
- 3 as [K.C.] kills herself.”
- 4 • After sending a nude photo of K.C. that appears to be one of the photos sent to U.S.
- 5 Navy inboxes, a text message was sent from the same number reading, “Did you
- 6 enjoy the pictures? I’ve spent the last two days emailing them to every single navy
- 7 email address I can get my hands on.”

8 23. In one of the voicemail messages to M.N. that I have reviewed, the caller

9 identified himself as “Christopher Crawford,” and said, in part, “I am not going to just burn

10 down Petty Officer Crawford’s house, I’m going to burn down the house of everyone who

11 gave her shelter...metaphorically speaking.” and “what do you fucking think I’m going to do

12 to any of you that fucking let her do this shit to me? Any of you that step between me and

13 my fucking child like that first command did, and I guarantee you I will make the act of

14 Congress happen necessary to get your fucking anchors in my god damned pocket!” In

15 another voicemail message, the caller identified himself as “Chris Crawford” and said, in

16 part, “Yeah, you keep going out and protecting her. And when she’s in prison, I’ll come after

17 all of you next!”

18 24. On December 15, 2021, Google was served with preservation letter under 18

19 U.S.C. § 2703(f) related to Google Voice phone numbers (401) 615-4218 and (786) 904-

20 3683.

21 25. Based on my review of the digital files provided by K.C., the nude/intimate

22 images of K.C. were posted to the Pornhub website by the Pornhub account with username

23 “skabb155.” Although Pornhub had removed the images prior my review, K.C. stated she

24 had already viewed the public website and confirmed the images were of her, before sending

25 a request to the Pornhub website to have them taken down. A grand jury subpoena to

26 Pornhub for subscriber information for the account “skabb155” revealed it to be registered to

27 “christopher crawford” with an email address “crawford132@gmail.com.” The subpoena

28 further revealed the account to have created two public photo albums: “US Navy, STG1, San

1 | Diego” (Album ID 61386732), and “US NAVY STG1, San Diego” (Album ID 61386822).
2 | “STG1” is the U.S. Navy designation for K.C.’s rating, that is, Sonar Technician (surface)
3 | Petty Officer 1st Class.

4 | 26. On November 24, 2021, MG Freesites, Ltd., the parent company that operates
5 | Pornhub, was served with a preservation letter under 18 U.S.C. § 2703(f) related to the
6 | “skabb155.”

7 | 27. Based on my interview of K.C. and my review of a digital photo provided by
8 | her, a foot massager purchased from Amazon.com was delivered to K.C.’s residence with a
9 | gift receipt bearing Order ID 111-4319768-1041835 and a transaction date of October 11,
10 | 2020, and stating it was from “c scott crawford.” The included gift message read, “Enjoy
11 | your gift! Happy early birthday. I hope this helps you relax so that you can focus on what is
12 | important and make better choices. I made promises I meant, even if you didn’t. From c scott
13 | crawford.” A grand jury subpoena to Amazon for subscriber information for the purchaser
14 | associated with that Order ID number revealed it to be registered to “c scott crawford” with
15 | an email address of “crawford132@gmail.com” and a billing address of “8620 8TH AVE W
16 | APT C, EVERETT, WA, US 98204-1640.” This communication came at a time when the
17 | Criminal Protective Order from San Diego County was in effect.

18 | 28. On December 3, 2021, Amazon was served with a preservation letter under 18
19 | U.S.C. § 2703(f) related to order identifier 111-4319768-1041835 and the account associated
20 | with that transaction.

21 | 29. Based on my interview of K.C. and my review of digital files provided by her,
22 | the user of the Facebook account with display name “Scott Crawford” (account identifier
23 | 100002445195272) sent harassing messages to K.C. Among the messages I have reviewed
24 | were an undated string of messages sent to K.C. between 4:09 a.m. and 4:58 a.m., that read
25 | as follows:

- 26 | • “What’s worse, using words to hurt someone or using childish, petty, vindictive
27 | actions to do the same?”
28 |

- “People will provoke you until they bring your ugly side, then play the victim when you go there.’ You are not the victim, stop trying to be.”

While the undated messages appear from their context to have been sent during the time period when C.S. CRAWFORD was restrained from contacting K.C., I cannot be certain., The requested warrant seeks information from Meta Platforms, Inc. that would assist my investigation by providing the precise date and context of these messages.

30. Additionally, based on the digital files provided by K.C., the “Scott Crawford” Facebook account also sent harassing messages to K.C.’s mother, J.C., that appear to be in violation of the lifetime restraining order against C.S. CRAWFORD issued by the District Court of Bexar County, Texas. I have reviewed a message from “Scott Crawford” to J.C. that reads as follows (certain references to individuals have been replaced with bracketed references based on my understanding of these individuals’ identities):

call your daughter. she has left me so you have gotten what you always wanted. If I find out that you are talking to [S.C.] though, I will be calling CPS on [K.C.] for the 4th time. She is already going to lose custody of [S.C.], don’t help her do it any more thoroughly
Dont forget that you are a pedophile, like your whole family. The [Guardian ad Litum for S.C.] has already ruled that you are a threat to [S.C.] and I have [K.C.’s] wills where she said she disowned you. YOu will never be allowed to be in a position where you can hurt my daughter like you did with your other kids, but you can still talk to your daughter. Granted, she has become a stupid, irresponsible, abusive, negligent, evil waste of life, but taht is why I feel you two will get along better now.

31. A grand jury subpoena to Facebook, Inc. for subscriber information for the “Scott Crawford” Facebook account revealed it to be registered to “Scott Crawford” with a verified phone number of (512) 667-5926 (verified on August 22, 2022), and a registered email address of “crawford132@hotmail.com.”

32. Based on my interview with K.C. and my review of digital files provided by her, the Facebook account with display name “Christopher Crawford” (account identifier 100054164457078) sent harassing messages to J.C. contemporaneously with the messages from the “Scott Crawford” account. Among other things, the messages accused J.C. of being

1 a “pedophile” and claimed that K.C. was now a convicted criminal with over 30 more
2 charges pending. Records checks conducted through the National Crime Information Center
3 (NCIC), State Regional & Federal Enterprise Retrieval System III (SRFERS), and
4 Department of Defense Law Enforcement Defense Data Exchange (D-DEx) databases
5 revealed no criminal history for K.C. A check conducted through the Defense Information
6 System for Security (DISS) database revealed K.C. remains eligible for a Sensitive
7 Compartmented Information (SCI) clearance designation, which is the highest security
8 clearance designation in the U.S. Government. A grand jury subpoena to Facebook, Inc. for
9 subscriber information for the “Christopher Crawford” account revealed it to be registered to
10 “Christopher Crawford” with a verified phone number of (512) 667-5926, and an account
11 creation date of August 1, 2020.

12 33. On December 6, 2021, Facebook, Inc. (now Meta Platforms, Inc.) was served
13 with a preservation letter under 18 U.S.C. § 2703(f) related to Facebook account identifiers
14 100002445195272 (username Scott Crawford), 100054164457078 (username Christopher
15 Crawford), and 100074078874761 (username Rick Johnston).

16 34. Based on my interview with K.C. and my review of digital files provided by
17 her, the Instagram account cscottcrawford (account identifier 27235979350) made a
18 harassing public comment on a public Instagram post made by K.C. The public comment
19 stated, “She wrote me this on 4/07/2018” along with a digital image appearing to be a
20 photograph of a computer screen displaying text. Among the text included the following,
21 purportedly a private message written by K.C. to C.S. CRAWFORD on a previous date,
22 reading, in part, “...about trying to make myself better and stronger, more decisive for you
23 and [S.C.]. I’m supposed to be the head of household and I can barely stand up for myself or
24 how many times I feel like I let you down because I don’t want to try something new with
25 you or that I wouldn’t let you treat me.” A grand jury subpoena to Facebook, Inc. for
26 subscriber information for this account revealed it to be registered to “Scott Crawford” with
27 a verified phone number of (512) 667-5926.
28

35. Based on my interview with K.C. and my review of digital files provided by her, the Instagram account `im_not_broken_just_very_sad` (account identifier 27605029014) sent multiple harassing messages to K.C. and public comments on her posts. Among the messages I have reviewed, an undated string of messages sent to K.C. included the following, apparently posted in the guise of an anonymous third party: "...he feels like his mother is emperor palpatine and you are anakin Skywalker. He feels like padme in the sense that you are turning to the dark side and it is breaking his heart. To side with her over him after everything she has done is almost too much for him to bear and the fact that you left [S.C.] with her instead of him is infuriating to him," and "...from his point of view you are the aggressor, not the victim; you have everything and he is begging for mercy scraps. He truly feels manipulated and baited by you, he feels you played him and then betrayed ever promise you ever made to him." Among the public comments I have reviewed included the following, also written in the guise of an anonymous third party: "And I like how you say 'time to grow' like you are the same wrist cutting, medicated sex toy for a married couple, flunking out of college, wanting to get two full arm sleeves and a dozen piercings, sleeping with a husband and wife, your gay boyfriend, and then seducing your future husband by telling him you were single, that you were when scott first found you sleeping in the parking lot of the college. Good think you are away from him and can 'grow,'" and "Good luck with a career as a sub hunter when you cant serve on a ship... You are not a good person. Everything you knew about being good came from him and like a 14 year old, hes no longer around so in your messed up head, nothing he ever said was true." A grand jury subpoena to Facebook, Inc. for subscriber information for this account revealed it to be registered to "scott crawford." The email address associated with the account is "endless sadness15@gmail.com," and the account was registered on January 1, 2020.

36. On December 6, 2021, Facebook, Inc. (now Meta Platforms, Inc.) was served with a preservation letter under 18 U.S.C. § 2703(f) related to Instagram account identifiers 27235979350 and 27605029014.

BACKGROUND REGARDING GOOGLE'S SERVICES³

37. Google is a suite of services owned by Google LLC, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Google's Gmail service provides its subscribers internet-based accounts that allow them to send, receive, and store emails online. Google accounts are typically identified by a single username, which serves as the subscriber's default email address, but which can also function as a subscriber's username for other Google services, such as instant messages and remote photo or file storage. All users of any Google service are internally identified by a numerical account identifier.

38. Based on my training and experience, I know that Google allows subscribers to obtain accounts by registering on Google's website. During the registration process, Google asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate email address for backup purposes, a phone number, and in some cases a means of payment. Google typically does not verify subscriber names. However, Google does verify the email address or phone number provided.

39. Once a subscriber has registered an account, Google provides email services that typically include folders such as an "inbox?" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. Google subscribers can also use that same username or account in connection with other services provided by Google.⁴

³ The information in this section is based on information published by Google on its website, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

⁴ Here, Google's other services may include electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps

1 40. In general, user-generated content (such as email, SMS text messages, and
2 voicemails) that are written using, stored on, sent from, or sent to a Google account can be
3 permanently stored in connection with that account, unless the subscriber deletes the
4 material. For example, if the subscriber does not delete an email, the email can remain on
5 Google's servers indefinitely. Even if the subscriber deletes the email, it may continue to
6 exist on Google's servers for a certain period of time.

7 41. Thus, a subscriber's Google account can be used not only for email but also for
8 other types of electronic communication, including instant messaging and photo and video
9 sharing; voice calls, voicemails, video chats, SMS text messaging; social networking.
10 Depending on user settings, user-generated content derived from many of these services is
11 normally stored on Google's servers until deleted by the subscriber. Similar to emails, such
12 user-generated content can remain on Google's servers indefinitely if not deleted by the
13 subscriber, and even after being deleted, it may continue to be available on Google's servers
14 for a certain period of time. Furthermore, a Google subscriber can store telephone call data,
15 voicemails, SMS text messages, contacts, calendar data, images, videos, notes, documents,
16 bookmarks, web searches, browsing history, and various other types of information on
17 Google's servers. Based on my training and experience, I know that the types of data
18 discussed above can include records and communications that constitute evidence of the
19 offenses of stalking and obscene or harassing telephone calls in interstate communications.

20 42. Based on my training and experience, I know that providers such as Google
21 also collect and maintain information about their subscribers, including information about
22 their use of Google services. This information can include the date on which the account was
23 created, the length of service, records of log-in (i.e., session) times and durations, the types
24 of service utilized, the status of the account (including whether the account is inactive or

25 _____
26 with driving directions and local business search) and other location services, and Language Tools
27 (text translation); online tracking and advertising tools such as Google Analytics (tracking and
28 reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel
Phone (services which support a Google smartphone); and Google Play (which allow users to
purchase and download digital content, e.g., applications).

1 closed), the methods used to connect to the account (such as logging into the account via the
2 provider's website), and other log files that reflect usage of the account. Providers such as
3 Google also commonly have records of the Internet Protocol address ("IP address") used to
4 register the account and the IP addresses associated with other logins to the account. Because
5 every device that connects to the Internet must use an IP address, IP address information can
6 help to identify which devices were used to access the relevant account. Also, providers such
7 as Google typically collect and maintain location data related to subscriber's use of Google
8 services, including data derived from IP addresses and/or Global Positioning System
9 ("GPS") data.

10 43. Based on my training and experience, I know that providers such as Google
11 also collect information relating to the devices used to access a subscriber's account – such
12 as laptop or desktop computers, cell phones, and tablet computers. Such devices can be
13 identified in various ways. For example, some identifiers are assigned to a device by the
14 manufacturer and relate to the specific machine or "hardware," some identifiers are assigned
15 by a telephone carrier concerning a particular user account for cellular data or voice services,
16 and some identifiers are actually assigned by Google in order to track what devices are using
17 Google's accounts and services. Examples of these identifiers include unique application
18 number, hardware model, operating system version, Global Unique Identifier ("GUID"),
19 device serial number, mobile network information, telephone number, Media Access Control
20 ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my
21 training and experience, I know that such identifiers may constitute evidence of the crimes
22 under investigation because they can be used (a) to find other Google accounts created or
23 accessed by the same device and likely belonging to the same user, (b) to find other types of
24 accounts linked to the same device and user, and (c) to determine whether a particular device
25 recovered during course of the investigation was used to access the Google account.

26 44. Google also allows its subscribers to access its various services through
27 applications that can be installed on and accessed via cellular telephones and other mobile
28 devices. These applications are associated with the subscriber's Google account. In my

1 training and experience, I have learned that when the user of a mobile application installs and
2 launches the application on a device (such as a cellular telephone), the application directs the
3 device in question to obtain a Push Token, a unique identifier that allows the provider
4 associated with the application (such as Google) to locate the device on which the
5 application is installed. After the applicable push notification service (e.g. Google Cloud
6 Messaging) sends a Push Token to the device, the Token is then sent to the application,
7 which in turn sends the Push Token to the application's server/provider. Thereafter,
8 whenever the provider needs to send notifications to the user's device, it sends both the Push
9 Token and the payload associated with the notification (i.e., the substance of what needs to
10 be sent by the application to the device). To ensure this process works, Push Tokens
11 associated with a subscriber's account are stored on the provider's server(s). Accordingly,
12 the computers of Google are likely to contain useful information that may help to identify the
13 specific device(s) used by a particular subscriber to access the subscriber's Google account
14 via the mobile application.

15 45. Based on my training and experience, I know that providers such as Google
16 use cookies and similar technologies to track users visiting Google webpages and using its
17 products and services. Basically, a "cookie" is a small file containing a string of characters
18 that a website attempts to place onto a user's computer. When that computer visits again, the
19 website will recognize the cookie and thereby identify the same user who visited before. This
20 sort of technology can be used to track users across multiple websites and online services
21 belonging to Google. More sophisticated cookie technology can be used to identify users
22 across devices and web browsers. From training and experience, I know that cookies and
23 similar technology used by providers such as Google may constitute evidence of the criminal
24 activity under investigation. By linking various accounts, devices, and online activity to the
25 same user or users, cookies and linked information can help identify who was using a Google
26 account and determine the scope of criminal activity.

27 46. Based on my training and experience, I know that Google maintains records
28 that can link different Google accounts to one another, by virtue of common identifiers, such

1 as common email addresses, common telephone numbers, common device identifiers,
2 common computer cookies, and common names or addresses, that can show a single person,
3 or single group of persons, used multiple Google accounts. Based on my training and
4 experience, I also know that evidence concerning the identity of such linked accounts can be
5 useful evidence in identifying the person or persons who have used a particular Google
6 account.

7 47. Based on my training and experience, I know that subscribers can
8 communicate directly with Google about issues relating to the account, such as technical
9 problems, billing inquiries, or complaints from other users. Providers such as Google
10 typically retain records about such communications, including records of contacts between
11 the user and the provider's support services, as well records of any actions taken by the
12 provider or user as a result of the communications. In my training and experience, such
13 information may constitute evidence of the crimes under investigation because the
14 information can be used to identify the account's user or users.

15 48. In summary, based on my training and experience in this context, I believe that
16 the computers of Google are likely to contain user-generated content such as stored
17 electronic communications (including retrieved and un-retrieved email, SMS text messages,
18 and voicemail), photos, videos, documents, and internet searches, as well as Google-
19 generated information about its subscribers and their use of Google services and other online
20 services (such as call data records). In my training and experience, all of that information
21 may constitute evidence of the offenses of stalking and harassing telephone calls in interstate
22 communications because the information can be used to identify the account's user or users.
23 In fact, even if subscribers provide Google with false information about their identities, that
24 false information often nevertheless provides clues to their identities, locations, or illicit
25 activities.

26 49. As explained above, information stored in connection with a Google account
27 may provide crucial evidence of the "who, what, why, when, where, and how" of the
28 offenses of stalking and obscene or harassing telephone calls in interstate communications,

1 thus enabling the United States to establish and prove each element of the offense, or,
2 alternatively, to exclude the innocent from further suspicion.

3 50. Further, stored communications and files connected to a Google account may
4 provide direct evidence of the offense under investigation. For example, it may include
5 records of the threatening and harassing communications sent to K.C. and other individuals
6 as described above, records of photos sent during these communications, and other evidence
7 of the account user's attempts to locate and contact K.C. and others, such as internet
8 searches.

9 51. From my training and experience, I know that the information stored in
10 connection with a Google account can indicate who has used or controlled the account. This
11 "user attribution" evidence is analogous to the search for "indicia of occupancy" while
12 executing a search warrant at a residence. For example, email communications, contacts lists,
13 and images sent (and the data associated with the foregoing, such as date and time) may
14 indicate who used or controlled the account at a relevant time. Further, information
15 maintained by Google can show how and when the account was accessed or used. For
16 example, providers such as Google typically log the IP addresses from which users access
17 the account along with the time and date. By determining the physical location associated
18 with the logged IP addresses, investigators can understand the chronological and geographic
19 context of the Google account access and use relating to the criminal activity under
20 investigation. This geographic and timeline information may tend to either inculcate or
21 exculpate the person who controlled, used, and/or created the account. Additionally,
22 information stored at the user's account may further indicate the geographic location of the
23 account user at a particular time (e.g., location information integrated into an image or video
24 sent via email).

25 52. Finally, stored electronic data may provide relevant insight into the user's state
26 of mind as it relates to the offenses of stalking and harassing telephone calls in interstate
27 communications. For example, information in the Google account may indicate its user's
28 motive and intent to commit a crime (e.g., communications relating to the crime), or

consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

BACKGROUND REGARDING PORNHUB⁵

53. Pornhub is a service owned by MG Freesites Ltd., a Luxembourg company with offices in the United States and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Pornhub is free-access pornographic multimedia sharing site, accessible through the web, which allows visitors to view sexually explicit images and videos for free and optionally pay to view premium content created and distributed by major production studios.

54. Additionally, Pornhub allows users to upload their own sexually explicit content for the purposes of free or paid distribution to other users of the service. This uploaded content can range from amateur to professional in production value. Users uploading their own content typically provide descriptive titles to their images, videos, and albums to cause them appear in keyword searches. Each piece of content can also be given categories such as “blonde” so other users can quickly screen available media for their personal preferences.

55. Viewing free content on Pornhub does not require a visitor to log in, but most other actions require that a visitor register for an account. Pornhub collects basic contact information from users during the registration process. Additionally, users may input billing information to their account to conduct financial transactions with Pornhub for premium services. This information, which can later be changed by the user, may include the user’s name, contact e-mail addresses, credit card or bank account number, billing address (including city, state, and zip code), telephone numbers, and other personal identifiers. Pornhub keeps records of changes made to this information.

⁵ The information in this section is based on information published by MG Freesites Ltd. on its website, including, but not limited to, the following webpage: www.mindgeek.com/about.

1 56. For each Pornhub user, Pornhub collects and retains the content and other
2 records described above, sometimes even after it is changed by the user (including
3 usernames, phone numbers, email addresses, full names, privacy settings, email addresses,
4 and content uploaded).

5 57. In my training and experience, evidence of who was using Pornhub and from
6 where, and evidence related to the offense of cyberstalking may be found in the files and
7 records described above. For example, the stored communications and files connected to a
8 Pornhub account may provide direct evidence of the criminal acts under investigation. Based
9 on my training and experience, photos, videos, and their associated text descriptions are
10 often created and used in furtherance of stalking, and in this case, nude and intimate images
11 of K.C. were uploaded to the Pornhub website without K.C.'s consent.

12 58. In addition, the user's account activity, logs, stored electronic communications,
13 and other data retained by Pornhub can serve as user attribution evidence to indicate who has
14 used or controlled the account.

15 59. Account activity may also provide relevant insight into the account owner's
16 state of mind as it relates to the offenses under investigation. For example, information on
17 the account may indicate the owner's motive and intent to commit a crime (e.g., information
18 indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account
19 information in an effort to conceal evidence from law enforcement).

20 60. Therefore, Pornhub's servers are likely to contain stored electronic
21 communications and information concerning subscribers and their use of Pornhub. In my
22 training and experience, such information may constitute evidence of the offenses under
23 investigation that can be used to verify the account's user and the offending communications
24 suspected.

25 //

26 //

27 //

BACKGROUND CONCERNING AMAZON⁶

61. “Amazon” is a service owned by Amazon.com, Inc., a United States company. Although Amazon provides a wide variety of services, Amazon’s principal business is operating an online retail establishment selling an extensive variety of items for delivery to a user’s mailing address or other addresses specified by the purchaser. Amazon delivers these items by a variety of methods to include U.S. Postal Service, several commercial parcel services, and Amazon's own delivery personnel.

62. Additionally, Amazon allows users to purchase items as gifts for direct delivery to the gift recipient’s address. The purchaser must know and provide the gift recipient’s address to send them a gift. When this occurs, the item may be accompanied by a gift receipt and a short message written by the purchaser. Amazon does not normally notify gift recipients of the item in advance of the item’s delivery.

63. Amazon collects personal and contact information from users during the registration process. This information, some of which can later be changed by the user, may include the user’s name, telephone number, contact e-mail addresses, credit card or bank account number, mailing address (including city, state, and zip code), billing address (including city, state, and zip code), alternate shipping address, and other personal identifiers. Amazon keeps records of changes made to this information.

64. For each Amazon user, Amazon collects and retains the information about each of their purchases and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and content uploaded).

65. In my training and experience, evidence of who was using Amazon and from where, and evidence related to the offense of stalking, may be found in the files and records described above. This evidence may help establish the “who, what, why, when, where, and

⁶ The information in this section is based on information published by Amazon.com, Inc. on its website.

1 how” of the offense, thus enabling the United States to establish and prove each element or,
2 alternatively, to exclude the innocent from further suspicion.

3 66. Therefore, Amazon’s servers are likely to contain stored electronic
4 communications and information concerning subscribers and their use of Amazon. In my
5 training and experience, such information may constitute evidence of the offenses under
6 investigation that can be used to verify the account’s user and the offending communications
7 suspected.

8 **BACKGROUND CONCERNING FACEBOOK AND INSTAGRAM⁷**

9 67. Facebook and Instagram are services owned by Mega Platforms, Inc., a United
10 States company and a provider of an electronic communications service as defined by 18
11 U.S.C. §§ 3127(1) and 2510. Specifically, Facebook and Instagram are free-access social
12 networking services, accessible through their websites and its mobile applications, that allow
13 subscribers to acquire and use Facebook and Instagram accounts, like the target account(s)
14 listed in Attachment A-4, through which users can share messages, multimedia, and other
15 information with other Facebook and Instagram users and the general public.

16 68. Mega Platforms, Inc. collects basic contact and personal identifying
17 information from users during the Facebook and Instagram registration processes. This
18 information, which can later be changed by the user, may include the user’s full name, birth
19 date, gender, contact e-mail addresses, physical address (including city, state, and zip code),
20 telephone numbers, credit card or bank account number, and other personal identifiers.
21 Facebook, Inc. keeps records of changes made to this information.

22 69. Mega Platforms, Inc. also collects and retains information about how each user
23 accesses and uses Facebook and Instagram. This includes information about the Internet
24

25 ⁷ The information in this section is based on information published by Facebook on its website and
26 on the Instagram website, including, but not limited to, the following webpages:
27 facebook.com/help/789682591639542 (“Help Center”), facebook.com/privacy/explanation (“Data
28 Policy”), facebook.com/safety/groups/law/guideline (“Information for Law Enforcement”),
help.instagram.com/519522125107875 (“Data Policy”), help.instagram.com/494561080557017
 (“Information for Law Enforcement”), and help.instagram.com (“Help Center”).

1 Protocol (“IP”) addresses used to create and use an account, unique identifiers and other
2 information about devices and web browsers used to access an account, and session times
3 and durations.

4 70. Each Facebook account is identified internally by a unique account identifier.
5 Externally, each Facebook account is identified to other users by a display name chosen by
6 the user. Facebook’s terms of service require the display name to be the user’s legal name,
7 however in practice this is commonly disobeyed. Users can change their display names
8 whenever they choose and there can be many duplicate display names. The account identifier
9 never changes regardless of changes to the display name.

10 71. Each Instagram account is identified by a unique username chosen by the user.
11 Users can change their usernames whenever they choose but no two users can have the same
12 usernames at the same time. Instagram users can create multiple accounts and, if “added” to
13 the primary account, can switch between the associated accounts on a device without having
14 to repeatedly log-in and log-out.

15 72. Users of both services can also connect their Instagram and Facebook accounts
16 together to utilize certain cross-platform features, and multiple Instagram accounts can be
17 connected to a single Facebook account. Instagram accounts can also be connected to certain
18 third-party websites and mobile apps for similar functionality. For example, an Instagram
19 user can “tweet” an image uploaded to Instagram to a connected Twitter account or post it to
20 a connected Facebook account, or transfer an image from Instagram to a connected image
21 printing service. Meta Platforms, Inc. maintains records of changed Instagram usernames,
22 associated Instagram accounts, and previous and current connections with accounts on
23 Facebook and third-party websites and mobile apps.

24 73. Facebook and Instagram users can “follow” other users to receive updates
25 about their posts and to gain access that might otherwise be restricted by privacy settings (for
26 example, users can choose whether their posts are visible to anyone or only to their
27 followers). Users can also “block” other users from viewing their posts and searching for
28 their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain

1 activity and prescreen their comments. Instagram also allows users to create a “close friends
2 list” for targeting certain communications and activities to a subset of followers.

3 74. Facebook and Instagram have several ways to search for friends and associates
4 to “friend” or “follow” on the platforms, such as by allowing Facebook or Instagram to
5 access the contact lists on their devices to identify which contacts are Facebook or Instagram
6 users. Meta Platforms, Inc. retains this contact data unless deleted by the user and
7 periodically syncs with the user’s devices to capture changes and additions. Users can
8 similarly allow Facebook or Instagram to search an associated Facebook or Instagram
9 account for friends who are also users of the platform. Users can also manually search for
10 friends or associates.

11 75. Each Facebook and Instagram user has a profile page where certain content
12 they create and share (“posts”) can be viewed either by the general public or only the user’s
13 followers, depending on privacy settings. Instagram users can customize their profile by
14 adding their name, a photo, a short biography (“Bio”), and a website address. Facebook users
15 can customize their profile with many more attributes than on Instagram.

16 76. One of Facebook and Instagram’s primary features is the ability to create, edit,
17 share, and interact with text, web links, photos, and short videos. Users can upload photos or
18 videos taken with or stored on their devices, to which they can apply filters and other visual
19 effects, add a caption, enter the usernames of other users (“tag”), or add a location. These
20 appear as posts or photo albums on the user’s profile. Users can remove posts from their
21 profiles by deleting or archiving them. Archived posts can be reposted because, unlike
22 deleted posts, they remain on Meta Platform, Inc.’s servers.

23 77. Users can interact with posts by liking them, adding or replying to comments,
24 or sharing them within or outside of Facebook or Instagram. Users receive notification when
25 they are tagged in a post by its creator or mentioned in a comment (users can “mention”
26 others by adding their username to a comment followed by “@”). A Facebook and Instagram
27 post created by one user may appear on the profiles or feeds of other users depending on a
28 number of factors, including privacy settings and which users were tagged or mentioned.

1 78. An Instagram “story” is similar to a post but can be viewed by other users for
2 only 24 hours. Stories are automatically saved to the creator’s “Stories Archive” and remain
3 on Meta Platform, Inc.’s servers unless manually deleted. The usernames of those who
4 viewed a story are visible to the story’s creator until 48 hours after the story was posted.

5 79. Facebook and Instagram allows users to broadcast live video from their
6 profiles. Viewers can like and add comments to an Instagram video while it is live, but the
7 video and any user interactions are removed from Instagram upon completion unless the
8 creator chooses to send the video to IGTV, Instagram's long-form video app. On Facebook,
9 the video and user interactions are generally available afterward indefinitely.

10 80. Facebook Messenger and Instagram Direct, the respective services’ messaging
11 functions, allows users to send private messages to select individuals or groups. These
12 messages may include text, photos, videos, posts, videos, profiles, and other information.
13 Participants to a group conversation can name the group and send invitations to others to
14 join. Facebook and Instagram users can send individual or group messages with
15 “disappearing” photos or videos that can only be viewed by recipients for a certain amount
16 of time, depending on settings. Senders can’t view their disappearing messages after they are
17 sent but do have access to each message’s status, which indicates whether it was delivered,
18 opened, or replayed, and if the recipient took a screenshot. Facebook Messenger and
19 Instagram Direct also enables users to video chat with each other directly or in groups.

20 81. Facebook and Instagram offer services such as Facebook Pay and Instagram
21 Checkout for users to make purchases, donate money, and conduct other financial
22 transactions within the respective platforms as well as on other associated websites and apps.
23 Facebook, Inc. collects and retains payment information, billing records, and transactional
24 and other information when these services are utilized.

25 82. Facebook and Instagram have search functions which allow users to search for
26 accounts by username, user activity by location, and user activity by hashtag. Hashtags,
27 which are topical words or phrases preceded by a pound sign (#), can be added to posts to
28 make them more easily searchable and can be “followed” to generate related updates from

1 Facebook or Instagram. Meta Platforms, Inc. retains records of a user's search history and
2 followed hashtags.

3 83. Meta Platforms, Inc. collects and retains location information relating to the
4 use of a Facebook or Instagram account, including user-entered location tags and location
5 information used by Facebook, Inc. to personalize and target advertisements.

6 84. Meta Platforms, Inc. uses information it gathers from its platforms and other
7 sources about the demographics, interests, actions, and connections of its users to select and
8 personalize ads, offers, and other sponsored content. Meta Platforms, Inc. maintains related
9 records for Facebook and Instagram users, including information about their perceived ad
10 topic preferences, interactions with ads, and advertising identifiers. This data can provide
11 insights into a user's identity and activities, and it can also reveal potential sources of
12 additional evidence.

13 85. In some cases, Facebook and Instagram users may communicate directly with
14 Meta Platforms, Inc. about issues relating to their accounts, such as technical problems,
15 billing inquiries, or complaints from other users. Social networking providers like Meta
16 Platforms, Inc. typically retain records about such communications, including records of
17 contacts between the user and the provider's support services, as well as records of any
18 actions taken by the provider or user as a result of the communications.

19 86. For each Facebook or Instagram user, Meta Platforms, Inc. collects and retains
20 the content and other records described above, sometimes even after it is changed by the user
21 (including usernames, phone numbers, email addresses, full names, privacy settings, email
22 addresses, and profile bios and links).

23 87. In my training and experience, evidence of who was using Facebook or
24 Instagram and from where, and evidence related to the offense of stalking, may be found in
25 the files and records described above. This evidence may establish the "who, what, why,
26 when, where, and how" of the criminal conduct under investigation, thus enabling the United
27 States to establish and prove each element or, alternatively, to exclude the innocent from
28 further suspicion.

1 88. For example, the stored communications and files connected to a Facebook or
2 Instagram account may provide direct evidence of the alleged stalking under investigation.
3 Based on my training and experience, direct messages, posts, photos, videos, and friend
4 requests are often created and used in furtherance of the offense of stalking. In this case,
5 there is probably cause to believe that C.S. CRAWFORD used these services to send
6 harassing messages as part of a pattern of cyberstalking.

7 89. In addition, the user's account activity, logs, stored electronic communications,
8 and other data retained by Facebook can indicate who has used or controlled the account. As
9 with the other providers of remote computing services discussed above, this "user
10 attribution" evidence is analogous to the search for "indicia of occupancy" while executing a
11 search warrant at a residence. For example, subscriber information, hardware and software
12 identifier information, and Internet Protocol (IP) address information (and the data associated
13 with the foregoing, such as geo-location, date and time), may be evidence of who used or
14 controlled the account at a relevant time. As an example, because every device has unique
15 hardware and software identifiers, and because every device that connects to the Internet
16 must use an IP address, IP address and device identifier information can help to identify
17 which computers or other devices were used to access the account. Such information also
18 allows investigators to understand the geographic and chronological context of access, use,
19 and events relating to the offense of stalking.

20 90. Account activity may also provide relevant insight into the account owner's
21 state of mind as it relates to the offenses under investigation. For example, information on
22 the account may indicate the owner's motive and intent to commit a crime (e.g., information
23 indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account
24 information in an effort to conceal evidence from law enforcement).

25 91. Other information connected to the use of Facebook and Instagram may lead to
26 the discovery of additional evidence. For example, the direct messages can lead to the
27 identification of additional acts of stalking not previously suspected.
28

1 92. Therefore, Facebook, Inc.'s servers are likely to contain stored electronic
2 communications and information concerning subscribers and their use of Facebook and
3 Instagram. In my training and experience, such information may constitute evidence of the
4 offense of cyberstalking including information that can be used to verify the account's user
5 and the offending communications suspected.

6 93. At times, providers of internet-based services, such as Google, Amazon,
7 Facebook, Instagram, and Pornhub, can and do change the details and functionality of the
8 services they offer. While the information in this section is true and accurate to the best of
9 my knowledge and belief, I have not specifically reviewed every detail of these providers'
10 services in connection with submitting this application for a search warrant. Instead, I rely
11 upon my training and experience, and the training and experience of others, to set forth the
12 foregoing description for the Court.

13 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

14 94. Pursuant to Title 18, United States Code, Section 2703(g), this application and
15 affidavit for a search warrant seeks authorization to permit the providers, and their agents
16 and employees, to assist agents in the execution of this warrant. Once issued, the search
17 warrant will be presented to the providers with direction that they identify the providers'
18 accounts described in Attachment A to this affidavit, as well as other subscriber and log
19 records associated with the accounts, as set forth in Section I of Attachment B to this
20 affidavit.

21 95. The search warrant will direct the providers to create an exact copy of the
22 specified account and records.

23 96. I, and/or other law enforcement personnel will thereafter review the copy of
24 the electronically stored data, and identify from among that content those items that come
25 within the items identified in Section II to Attachment B, for seizure.

26 97. Analyzing the data contained in the forensic image may require special
27 technical skills, equipment, and software. It could also be very time-consuming. Searching
28 by keywords, for example, can yield thousands of "hits," each of which must then be

1 reviewed in context by the examiner to determine whether the data is within the scope of the
2 warrant. Merely finding a relevant “hit” does not end the review process. Keywords used
3 originally need to be modified continuously, based on interim results. Certain file formats,
4 moreover, do not lend themselves to keyword searches, as keywords, search text, and many
5 common email, database and spreadsheet applications do not store data as searchable text.
6 The data may be saved, instead, in proprietary non-text format. And, as the volume of
7 storage allotted by service providers increases, the time it takes to properly analyze
8 recovered data increases, as well. Consistent with the foregoing, searching the recovered data
9 for the information subject to seizure pursuant to this warrant may require a range of data
10 analysis techniques and may take weeks or even months. All forensic analysis of the data
11 will employ only those search protocols and methodologies reasonably designed to identify
12 and seize the items identified in Section II of Attachment B to the warrant.

13 98. Based on my experience and training, and the experience and training of other
14 agents with whom I have communicated, it is necessary to review and seize a variety of
15 email communications, chat logs and documents, that identify any users of the subject
16 account and emails sent or received in temporal proximity to incriminating emails that
17 provide context to the incriminating communications.

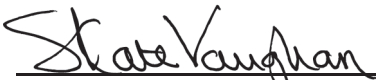
18 CONCLUSION

19 99. Based on the forgoing, I request that the Court issue the proposed search
20 warrant. This Court has jurisdiction to issue the requested warrant because it is “a court of
21 competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) &
22 (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that - has
23 jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18
24 U.S.C. § 2703(g), the government will execute this warrant by serving the warrant on the
25 providers. Because the warrant will be served on the providers, who will then compile the
26 requested records and data, reasonable cause exists to permit the execution of the requested
27 warrant at any time in the day or night. Accordingly, by this Affidavit and Warrant, I seek
28 authority for the government to search all of the items specified in Section I, Attachment B

1 (attached hereto and incorporated by reference herein) to the Warrant, and specifically to
2 seize all of the data, documents and records that are identified in Section II to that same
3 Attachment.

4
5 
6 EDDY CROCHETIERE, Affiant
7 Special Agent
8 Naval Criminal Investigative Service

9 The above-named agent provided a sworn statement attesting to the truth of the
10 contents of the foregoing affidavit by telephone on this 2nd day of March, 2022.

11
12 
13 S. KATE VAUGHAN
14 United States Magistrate Judge
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A-1

Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the Google accounts with the following identifiers:

crawford132@gmail.com (active on, but not limited to, October 27, 2021)

rickjohnston1888@gmail.com (active on, but not limited to, November 3, 2021)

endless sadness15@gmail.com (active on, but not limited to, January 1, 2020)

phone number +14016154218 (active on, but not limited to, July 30, 2020)

phone number +17869043683 (active on, but not limited to, October 29, 2021)

as well as all other subscriber and log records associated with the account, which are located at premises owned, maintained, controlled or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B-1**Section I - Information to be disclosed by Google LLC, for search:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google LLC (“the provider”), regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to the provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on November 24, 2021, December 15, 2021, February 18, 2022, and February 24, 2022, the provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

a. All content, records, and other information relating to communications sent from or received by the account(s) from April 1, 2019, to the present, including but not limited to:

i. The content of all communications sent from or received by the account(s), including emails, chats, SMS messages, voicemail recordings, and all associated multimedia and metadata, including deleted and draft content if available;

ii. All call data records and other information about Google Voice telephone usage by the accounts to/from the specified recipients, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as call answered, call not answered, call blocked, voicemail recorded);

iii. The source and destination addresses associated with each communication, the date and time sent or received, and the size and length of each email; and;

iv. All associated logs and metadata;

b. All records or other information regarding the identification of the account(s), to include full name, physical address, email address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number), and devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

1 c. All location information, including location history, login activity,
2 information geotags, and related metadata from April 1, 2019, to the present;

3 d. All Google usernames (past and current) and the date and time each
4 username was active, all associated Google accounts (including those linked by machine
5 cookie), and all records or other information about connections with Google, third-party
6 websites, and mobile apps (whether active, expired, or removed);

7 e. The types of service(s) utilized by the user;

8 f. All records or other information stored at any time by an individual
9 using the account, including address books, contact and buddy lists, calendar data, pictures,
10 videos, and files, from April 1, 2019, to the present;

11 g. Privacy and account settings, including change history; and

12 h. All records pertaining to communications between the provider and any
13 person regarding the account, including contacts with support services and records of actions
14 taken.

15 **The Provider is hereby ordered to disclose the above information to the government**
16 **within 14 days of issuance of this warrant.**

17
18 **Section II - Information to be seized by the government**

19 All information described above in Section I that constitutes evidence and
20 instrumentalities of violations of 18 U.S.C. § 2261A(2)(B) (cyberstalking) and 47 U.S.C.
21 § 223(a)(1)(E) (repeated harassing communications), those violations occurring April 1,
22 2019, to the present, including, for each account or identifier listed on Attachment A-1,
23 information pertaining to the following matters:

24 a. Communications and evidence of communications between the user of
25 the account(s) and any of the following: the individual identified in the search warrant
26 application as K.C., and any of her family, co-workers, or associates, including but not
27 limited to the individuals identified in the search warrant application as J.C., D.C, J.M., and
28 M.N.;

1 b. Evidence of the use of an interactive computer service, electronic
2 communications service, telephones, or the mail to harass, intimidate, or cause substantial
3 emotional distress to K.C., either directly or through family or associates;

4 c. Any images of K.C. in a partially or fully undressed state;

5 d. Evidence of the use of an interactive computer service, electronic
6 communications service, or the mail to share images of K.C. with any other individual,
7 website, interactive computer service, or members of the public;

8 e. Evidence of the placing of telephone calls with the intent to abuse,
9 threaten, or harass, either directly or indirectly, K.C., and any of her family, co-workers, and
10 associates, including the individuals identified as J.C., D.C, J.M. and M.N.;

11 f. Evidence indicating the account owner's state of mind as it relates to the
12 crimes under investigation;

13 g. All messages, documents, images, videos, profile information,
14 attachments, or other data that tends to identify any persons who use or access the account(s)
15 specified, or who exercise in any way any dominion or control over the specified account(s);

16 h. All messages, documents, profile information, logs, or other data that
17 tends to identify any device used to access the specified account(s), and any data tending to
18 identify the user or person who has access to any such device;

19 i. Any address lists, buddy lists, or lists of contacts associated with the
20 specified account(s).

21 j. All subscriber records associated with the specified account, including
22 name, address, local and long-distance telephone connection records, or records of session
23 times and durations, length of service (including start date) and types of service utilized,
24 telephone or instrument number or other subscriber number or identity, including any
25 temporarily assigned network address, and means and source of payment for such service,
including any credit card or bank account number;

26 k. Any and all other log records, including IP address captures, associated
27 with the specified account;
28

1 l. Any records of communications between the provider and any person
2 about issues relating to the account, such as technical problems, billing inquiries, or
3 complaints from other users about the specified account. This is to include records of
4 contacts between the subscriber and the provider's support services, as well as records of any
5 actions taken by the provider or subscriber as a result of the communications.

6 m. The identity of person(s) who communicated with the user of the
7 account(s) about matters relating to K.C., including records that help reveal their
8 whereabouts.

9 This warrant authorizes a review of electronically stored information, communications, other
10 records and information disclosed pursuant to this warrant in order to locate evidence and
11 instrumentalities described in this warrant. The review of this electronic data may be
12 conducted by any government personnel assisting in the investigation, who may include, in
13 addition to law enforcement officers and agents, attorneys for the government, attorney
14 support staff, and technical experts. Pursuant to this warrant, the Naval Criminal
15 Investigative Service (NCIS) may deliver a complete copy of the disclosed electronic data to
16 the custody and control of attorneys for the government and their support staff for their
17 independent review.
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A-2

Account to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the Pornhub account with the following identifier:

Skabb155 (active on, but not limited to, June 30, 2020)
as well as all other subscriber and log records associated with the account, which are located at premises owned, maintained, controlled or operated by MG Freesites Ltd, a company headquartered at 32 boulevard Royal, L-2449 Luxembourg City, Luxembourg, with offices located at 21800 Oxnard Street, Suite 150, Woodland Hills, CA 91367, and receiving process at 195-197 Old Nicosia-Limassol Road, Block 1 Dali Industrial Zone, Cyprus 2540.

ATTACHMENT B-2**Section I - Information to be disclosed by MG Freesites Ltd., for search:**

To the extent that the information described in Attachment A is within the possession, custody, or control of MG Freesites Ltd. (“the provider”), regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to MG Freesites Ltd., or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on November 24, 2021, MG Freesites Ltd. is required to disclose the following information to the government for the account listed in Attachment A-2:

- a. All business records and subscriber information, in any form kept, pertaining to the account, including:
 - i. Identity and contact information for any user of the account (past and present), including full name, email addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;
 - ii. All Pornhub user IDs or usernames (past and present), the date and time each user ID or username was active, and all records or other information about connections with third-party websites and mobile apps (whether active, expired, or removed);
 - iii. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;
 - iv. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
 - v. Internet Protocol (“IP”) addresses used to create, login, and use the account, including associated dates, times, and port numbers, from April 1, 2019, to the present;
 - vi. Privacy and account settings, including change history; and
 - vii. Communications between the provider and any person regarding the account, including contacts with support services, removal/takedown requests, and records of actions taken;
- b. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos, images, past and current bios and profiles, and all associated logs and metadata, from April 1, 2019 to the present, including but not limited to album IDs 61386822 and 61386732;

1 c. All records of searches performed by the account from April 1, 2019 to
2 the present;

3 d. All location information, including location history, login activity,
4 information geotags, and related metadata from April 1, 2019, to the present;

5 **The Provider is hereby ordered to disclose the above information to the government**
6 **within 14 days of issuance of this warrant.**

7 **Section II - Information to be seized by the government**

8 All information described above in Section I that constitutes evidence and
9 instrumentalities of violations of 18 U.S.C. § 2261A(2)(B) (cyberstalking) and 47 U.S.C.
10 § 223(a)(1)(E) (repeated harassing communications), those violations occurring April 1,
11 2019, to the present, including, for each account or identifier listed on Attachment A-2,
12 information pertaining to the following matters:

13 a. All subscriber records associated with the specified account, and
14 evidence of the identity of the person(s) who created or used the account, including name,
15 address, local and long-distance telephone connection records, or records of session times
16 and durations, length of service (including start date) and types of service utilized, telephone
17 or instrument number or other subscriber number or identity, including any temporarily
18 assigned network address, and means and source of payment for such service, including any
credit card or bank account number;

19 b. Evidence of the use of an interactive computer service or electronic
20 communications service to upload, publish, or share images of the individual identified in the
21 search warrant application as K.C.;

22 c. Evidence indicating how and when the account was accessed or used,
23 including evidence of the dates and times of access, methods used, device(s) used, IP
24 addresses used, and the location of the user, from April 1, 2019, to the present;

25 d. Any images of K.C.;

26 e. Evidence indicating the account owner's state of mind as it relates to the
27 crimes under investigation, from April 1, 2019, to the present;

1 f. Any records of communications between the provider and any person
2 about issues relating to the account, such as technical problems, billing inquiries, or
3 complaints from other users about the specified account. This is to include records of
4 contacts between the subscriber and the provider's support services, as well as records of any
5 actions taken by the provider or subscriber as a result of the communications.

6 This warrant authorizes a review of electronically stored information, communications, other
7 records and information disclosed pursuant to this warrant in order to locate evidence and
8 instrumentalities described in this warrant. The review of this electronic data may be
9 conducted by any government personnel assisting in the investigation, who may include, in
10 addition to law enforcement officers and agents, attorneys for the government, attorney
11 support staff, and technical experts. Pursuant to this warrant, the Naval Criminal
12 Investigative Service (NCIS) may deliver a complete copy of the disclosed electronic data to
13 the custody and control of attorneys for the government and their support staff for their
14 independent review.
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A-3

Account(s) to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Amazon Order ID 111-4319768-1041835 and the Amazon account associated with email address crawford132@gmail.com which are located at premises owned, maintained, controlled or operated by Amazon.com, Inc., a company headquartered at 410 Terry Ave N, Seattle, Washington 98109.

ATTACHMENT B-3**Section I - Information to be disclosed by Amazon.com, Inc. ("Amazon"), for search:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Amazon, regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to Amazon, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on December 3, 2021, and February 18, 2022, Amazon is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

- a. All business records and subscriber information, in any form kept, pertaining to the account, including:
 - i. Identity and contact information for any user of the account (past and present), including full name, email addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;
 - ii. All Amazon user IDs or usernames (past and present), the date and time each user ID or username was active, and all records or other information about connections with Amazon.com, third-party websites, and mobile apps (whether active, expired, or removed);
 - iii. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;
 - iv. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, apps and web browsers, and location data;
 - v. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from April 1, 2019, to the present;
 - vi. Privacy and account settings, including change history; and
 - vii. Communications between Amazon and any person regarding the account, including contacts with support services, removal/takedown requests, and records of actions taken;

- 1 b. All content, records, and other information relating to the transaction
 2 specified in Attachment A-3, including but not limited to:
 3 i. The items purchased, the identifier information of the sender, the
 4 identifier information of the recipient, any related gift message; and
 5 ii. All associated logs and metadata;
 6
 7 c. All location information, including location history, login activity,
 8 information geotags, and related metadata from the transaction specified in Attachment A-3.

9
 10 **The Provider is hereby ordered to disclose the above information to the government
 11 within 14 days of issuance of this warrant.**

12 **Section II - Information to be seized by the government**

13 All information described above in Section I that constitutes evidence and
 14 instrumentalities of violations of 18 U.S.C. § 2261A(2)(B) (cyberstalking) and 47 U.S.C.
 15 § 223(a)(1)(E) (repeated harassing communications), those violations occurring April 1,
 16 2019, to the present, including, for each account or identifier listed on Attachment A-1,
 17 information pertaining to the following matters:

18 a. Evidence of the use of an interactive computer service, electronic
 19 communications service, or the mail to contact, harass, intimidate, or cause substantial
 20 emotional distress to K.C., either directly or through family or associates;

21 b. All subscriber records associated with the specified account, including
 22 name, address, local and long-distance telephone connection records, or records of session
 23 times and durations, length of service (including start date) and types of service utilized,
 24 telephone or instrument number or other subscriber number or identity, including any
 25 temporarily assigned network address, and means and source of payment for such service,
 26 including any credit card or bank account number;

27 c. All messages, documents, profile information, logs, or other data that
 28 tend to identify any device used to access the specified account, and any data tending to
 identify the user or person who has access to any such device, and any data related to the
 location of the user;

1 d. Any and all other log records, including IP address captures, associated
2 with the specified account;

3 e. Any records of communications between Amazon and any person about
4 issues relating to the account, such as technical problems, billing inquiries, or complaints
5 from other users about the specified account. This is to include records of contacts between
6 the subscriber and the provider's support services, as well as records of any actions taken by
7 the provider or subscriber as a result of the communications.

8 This warrant authorizes a review of electronically stored information, communications, other
9 records and information disclosed pursuant to this warrant in order to locate evidence and
10 instrumentalities described in this warrant. The review of this electronic data may be
11 conducted by any government personnel assisting in the investigation, who may include, in
12 addition to law enforcement officers and agents, attorneys for the government, attorney
13 support staff, and technical experts. Pursuant to this warrant, the Naval Criminal
14 Investigative Service (NCIS) may deliver a complete copy of the disclosed electronic data to
15 the custody and control of attorneys for the government and their support staff for their
16 independent review.
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A-4

Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the Meta Platforms, Inc. accounts with the following identifiers:

Facebook account identifier 100002445195272 (active on, but not limited to, August 22, 2021)

Facebook account identifier 100054164457078 (active on, but not limited to, August 1, 2020)

Facebook account identifier 100074078874761 (active on, but not limited to, October 30, 2021)

Instagram account identifier 27235979350 (active on, but not limited to, October 30, 2021)

Instagram account identifier 27605029014 (active on, but not limited to, January 1, 2020)

as well as all other subscriber and log records associated with the account, which are located at premises owned, maintained, controlled or operated by Meta Platforms, Inc., a company headquartered at 1601 Willow Road, Menlo Park, California 94025.

ATTACHMENT B-4**Section I - Information to be disclosed by Meta Platforms, Inc., for search:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta Platforms, Inc. (“the provider”), regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to the provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on December 6, 2021, the provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-4:

a. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

b. All Facebook and Instagram display names/usernames (past and current) and the date and time each username was active, all associated Facebook and Instagram accounts (including those linked by machine cookie), and all records or other information about connections with the provider, third-party websites, and mobile apps (whether active, expired, or removed);

c. All activity logs for the account and all other documents showing the user’s posts and other Facebook activities from April 1, 2019 to present;

d. All photos and videos uploaded by that account and all photos and videos uploaded by any user that have that user tagged in them from April 1, 2019, to the present, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;

e. All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;

1 f. All content (whether created, uploaded, or shared by or with the
2 Account), records, and other information relating to videos (including live videos and videos
3 on IGTV), images, stories and archived stories, past and current bios and profiles, posts and
4 archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed
5 hashtags, shares, invitations, and all associated logs and metadata, from April 1, 2019, to the
6 present;

7 g. All records or other information regarding the devices and internet
8 browsers associated with, or used in connection with, that user ID, including the hardware
9 model, operating system version, unique device identifiers, mobile network information, and
10 user agent string;

11 h. All content, records, and other information relating to communications
12 sent from or received by the Account from April 1, 2019, to the present, including but not
13 limited to:

14 i. The content of all communications sent from or received by the
15 account(s), including direct and group messages, Messenger activity, public and private
16 messages, chat history, video and voice calling history, and pending "Friend" requests, and
17 all associated multimedia and metadata, including deleted and draft content if available;

18 ii. All records and other information about direct, group, and
19 disappearing messages sent from or received by the account(s), including dates and times,
20 methods, sources and destinations (including usernames and account numbers), and status
21 (such as delivered, opened, replayed, screenshot);

22 iii. Interactions by other Instagram users with the account(s) or
23 content thereof, including posts, comments, likes, tags, follows (including unfollows,
24 approved and denied follow requests, and blocks and unblocks), shares, invitations, and
25 mentions;

26 iv. All users the account has followed (including the close friends
27 list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of
28 users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a
request to follow the account

29 v. All records and other information about group conversations and
30 video chats, including dates and times, durations, invitations, and participants (including
31 usernames, account numbers, and date and time of entry and exit); and

32 vi. All associated logs and metadata;

33 i. All IP logs, including all records of the IP addresses that logged into the
34 account(s), from April 1, 2019, to the present;

1 j. All records of searches performed by the account(s) from April 1, 2019,
2 to the present;

3 k. The types of services utilized by the user;

4
5 l. The length of service (including start date) and the means and source of
6 any payments associated with the service (including any credit card or bank account
7 number);

8 m. All privacy settings and other account settings, including privacy
9 settings for individual Facebook and Instagram posts and activities, and all records showing
10 which Facebook and Instagram users have been blocked by the account(s);

11 n. All records pertaining to communications between the provider and any
12 person regarding the user or the user's account(s), including contacts with support services
13 and records of actions taken.

14 o. All location information, including location history, login activity,
15 information geotags, and related metadata from April 1, 2019, to the present.

16 **The Provider is hereby ordered to disclose the above information to the government**
17 **within 14 days of issuance of this warrant.**

18 **Section II - Information to be seized by the government**

19 All information described above in Section I that constitutes evidence and
20 instrumentalities of violations of 18 U.S.C. § 2261A(2)(B) (cyberstalking) and 47 U.S.C.
21 § 223(a)(1)(E) (repeated harassing communications), those violations occurring April 1,
22 2019, to the present, including, for each account or identifier listed on Attachment A-4,
23 information pertaining to the following matters:

24 a. Communications and evidence of communications between the user of
25 the account(s) and any of the following: the individual identified in the search warrant
26 application as K.C., and any of her family, co-workers, or associates, including but not
27 limited to the individuals identified in the search warrant application as J.C., D.C, J.M., and
28 M.N.;

1 b. Evidence of the use of an interactive computer service, electronic
2 communications service, telephones, or the mail to harass, intimidate, or cause substantial
3 emotional distress to K.C., either directly or through family or associates;

4 c. Any images of K.C. in a partially or fully undressed state;

5 d. Evidence of the use of an interactive computer service, electronic
6 communications service, or the mail to share images of K.C. with any other individual,
7 website, interactive computer service, or members of the public;

8 e. Evidence indicating the account owner's state of mind as it relates to the
9 crimes under investigation;

10 f. All messages, documents, images, videos, profile information,
11 attachments, or other data that tends to identify any persons who use or access the account(s)
12 specified, or who exercise in any way any dominion or control over the specified account(s);

13 g. All messages, documents, profile information, logs, or other data that
14 tends to identify any device used to access the specified account(s), and any data tending to
15 identify the user or person who has access to any such device, and the location of such user;

16 h. Any address lists, buddy lists, or lists of contacts associated with the
17 specified account(s).

18 i. All subscriber records associated with the specified account, including
19 name, address, local and long-distance telephone connection records, or records of session
20 times and durations, length of service (including start date) and types of service utilized,
21 telephone or instrument number or other subscriber number or identity, including any
22 temporarily assigned network address, and means and source of payment for such service,
including any credit card or bank account number;

23 j. Any and all other log records, including IP address captures, associated
24 with the specified account;

1 k. Any records of communications between the provider and any person
2 about issues relating to the account, such as technical problems, billing inquiries, or
3 complaints from other users about the specified account. This is to include records of
4 contacts between the subscriber and the provider's support services, as well as records of any
5 actions taken by the provider or subscriber as a result of the communications.

6 l. The identity of person(s) who communicated with the user of the
7 account(s) about matters relating to K.C., including records that help reveal their
8 whereabouts.

9 This warrant authorizes a review of electronically stored information, communications, other
10 records and information disclosed pursuant to this warrant in order to locate evidence and
11 instrumentalities described in this warrant. The review of this electronic data may be
12 conducted by any government personnel assisting in the investigation, who may include, in
13 addition to law enforcement officers and agents, attorneys for the government, attorney
14 support staff, and technical experts. Pursuant to this warrant, the Naval Criminal
15 Investigative Service (NCIS) may deliver a complete copy of the disclosed electronic data to
16 the custody and control of attorneys for the government and their support staff for their
17 independent review.
18
19
20
21
22
23
24
25
26
27
28

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [PROVIDER], and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of [PROVIDER]. The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of [PROVIDER], and they were made by [PROVIDER] as a regular practice; and

b. such records were generated by [PROVIDER'S] electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of [PROVIDER] in a manner to ensure that they are true duplicates of the original records; and

Date _____ Signature _____